SURFTECH

WHITE PAPER

Strategie avanzate di Backup e Restore: le nuove sfide e le soluzioni per le aziende

Sommario

Introduzione

In un mondo sempre più connesso e digitalizzato, i dati si sono affermati come una delle risorse più preziose per le aziende di ogni settore. La capacità di raccogliere, analizzare e sfruttare queste informazioni si traduce in vantaggi competitivi significativi, come l'ottimizzazione dei processi interni, una migliore comprensione del comportamento dei clienti e lo sviluppo di nuovi prodotti e servizi innovativi.
Di conseguenza, garantire la disponibilità, l'integrità e la confidenzialità dei dati è diventato un imperativo strategico per le organizzazioni che vogliono mantenere e rafforzare la loro posizione nel mercato.

Per questo motivo, le soluzioni di Backup e Restore sono fondamentali per prevenire e recuperare da eventuali perdite, danneggiamenti o attacchi informatici assicurando la continuità operativa.

Tuttavia, l'evoluzione tecnologica e il mutamento del panorama delle minacce richiedono un aggiornamento costante delle strategie di B&R. Con l'aumento della complessità delle infrastrutture IT e l'espansione del cloud computing, le aziende si trovano di fronte alla necessità di rivedere le proprie politiche di protezione dei dati. In questo contesto, è essenziale valutare la resilienza informatica aziendale, adattando le soluzioni di B&R alle nuove sfide, per garantire una gestione dei dati sicura e efficace nel lungo termine.

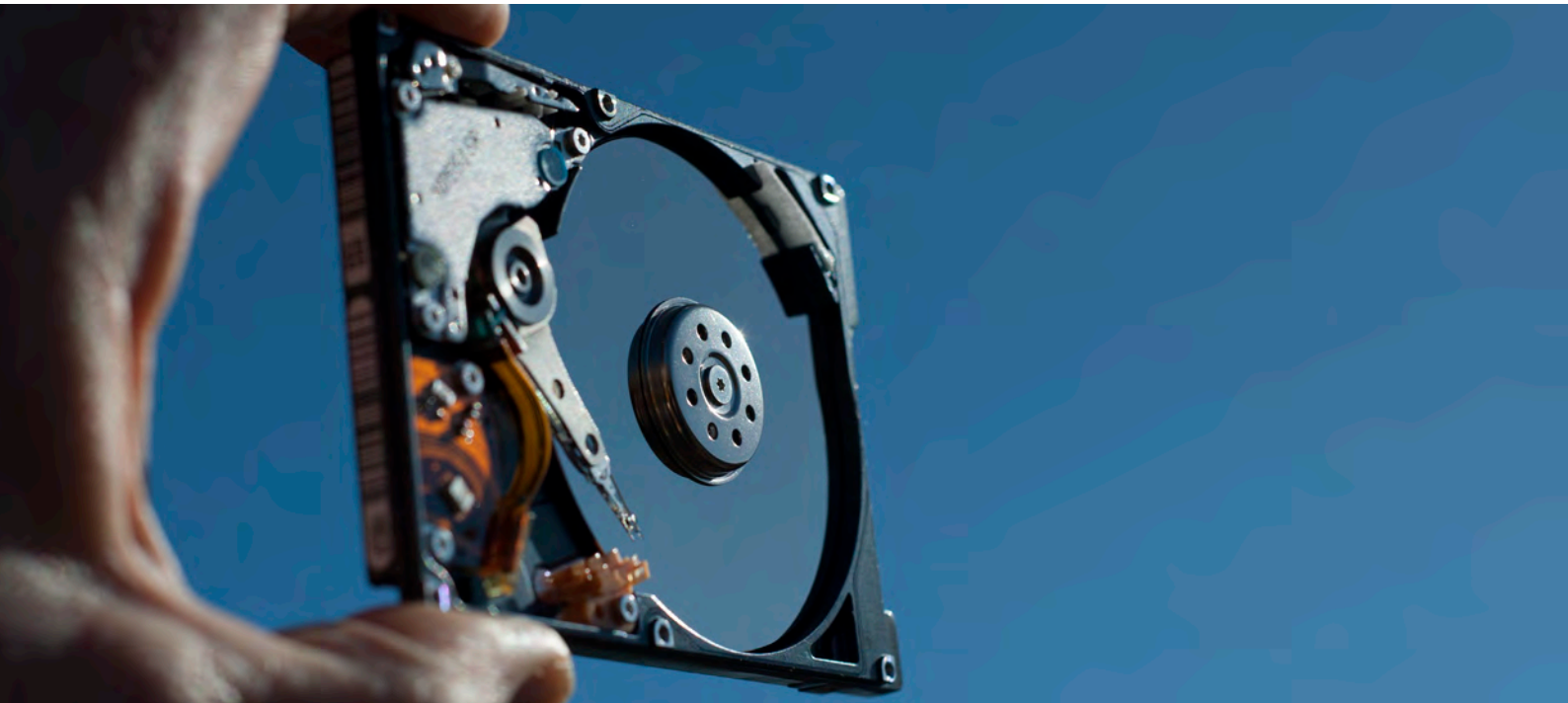
Le nuove sfide

Le principali sfide che le aziende devono oggi affrontare sono le seguenti:

Le aziende devono oggi tener presente che i loro dati si trovano distribuiti in sistemi e ambienti diversi - sia tradizionali che Cloud, su più sedi, sui dispositivi degli utenti, etc.. Per avere una soluzione di backup efficace, devono considerare queste diversità per non perdere dati rilevanti, gestire il processo con facilità e efficienza e adattarsi ai cambiamenti che si presentano.

Esistono criminali informatici che hanno come obiettivo principale l'ambiente di backup, al fine di renderlo inservibile prima di colpire i sistemi di produzione. In questo modo l'azienda è costretta a pagare il riscatto per recuperare i dati. È quindi essenziale usare delle strategie di sicurezza per difendere gli ambienti di backup dagli attacchi informatici.

L'aumento degli attacchi informatici aumenta l'importanza di saper ripristinare i dati nel minor tempo possibile e senza perdite: per questo è importante assicurarsi che i backup siano validi e coerenti, automatizzare le procedure di restore per evitare errori e ritardi, e dare la precedenza al recupero delle funzioni aziendali più critiche.



Le soluzioni disponibili

Per rispondere a queste sfide, il mercato ha reso disponibili soluzioni che indirizzano tali esigenze, tra cui:

Piattaforme sempre più ampie ed inclusive, con sistemi di licensing flessibili, che consentono di coprire tutte le fonti di dati con una soluzione unica e integrata.

Sistemi di protezione dei backup tramite storage immutabili, che impediscono la modifica o la cancellazione dei dati da parte di agenti esterni o interni.

Soluzioni storage che permettono di mantenere delle copie di backup dei dati direttamente sui sistemi di produzione, non visibili né alterabili ma disponibili per un rapido ripristino.

Soluzioni per l'orchestrazione e i test dei restore, che permettono di verificare periodicamente la funzionalità e la qualità dei backup e di automatizzare il processo di ripristino in caso di necessità.

Sistemi di rilevamento di anomalie nei backup, che avvisano in tempo reale di eventuali variazioni sospette nel volume o nella frequenza dei backup e soluzioni di protezione degli accessi tramite autenticazione a più fattori e richiesta di doppia conferma.

Individuazione dei dati e sistemi da proteggere

Per progettare o ri-progettare il proprio sistema di B&R è innanzitutto necessario effettuare una mappatura accurata del proprio ambiente informatico, identificando le fonti di dati, le tipologie di dati, le dimensioni dei dati, le modalità di accesso ai dati e le piattaforme su cui risiedono i dati.

Questa analisi può essere svolta con l'ausilio di strumenti di discovery automatizzati, che scansionano la rete e rilevano tutte le posizioni in cui sono presenti dei dati, e manualmente, tramite interviste agli utenti, revisione della documentazione e verifica delle configurazioni.

Alcune domande utili per guidare il processo di individuazione dei dati sono:

Dove sono archiviati i dati? Si trovano su server locali, storage centralizzato, storage locale, cloud pubblico, cloud privato, desktop, laptop, tablet, smartphone, etc.?

Quali sono le caratteristiche dei dati? Qual è la frequenza di modifica dei dati? Qual è la dimensione dei dati? I dati sono compressi o cifrati?

Come vengono utilizzati i dati? Chi accede ai dati e con quali permessi? Quali sono le dipendenze tra i dati e le applicazioni? Quali sono i requisiti di performance e disponibilità dei dati? Quali sono i livelli di servizio richiesti per i dati?

Questa analisi va fatta con regolarità e in profondità, perché spesso gli utenti non sanno quali pericoli corrono i loro dati, danno per scontato che siano al sicuro e non badano a dove li memorizzano, senza seguire le norme aziendali.

In più, in azienda ci possono essere anche apparati specifici, come NAS, switch, router, dispositivi di produzione, che hanno dati e configurazioni da salvare e che vengono talvolta introdotti in azienda senza darne adeguata comunicazione a chi si occupa dei backup.

Per mitigare questo problema, alcune soluzioni possono essere configurate in modo che ogni nuovo elemento creato in quell'ambiente, come una Virtual Machine, una Mailbox o un database, sia incluso automaticamente nei piani di backup predefiniti.

Classificazione dei dati

L'identificazione dell'importanza e della criticità dei dati per il business permette di adottare soluzioni e configurazioni di Backup e Restore più sofisticate e costose solo per i dati che effettivamente lo richiedono. Inoltre consente di stabilire delle priorità nelle operazioni di ripristino in caso di emergenza.

Per classificare i dati in base all'importanza e alla criticità per il business, è possibile utilizzare diversi criteri, come:

- Il valore dei dati per le attività core dell'azienda, come la produzione, la vendita o la logistica;
- il tempo necessario per ricreare i dati in caso di perdita o corruzione, e la fattibilità di tale operazione;
- la sensibilità e la confidenzialità dei dati, e le possibili conseguenze legali o
- reputazionali in caso di violazione;
- la frequenza di modifica e aggiornamento dei dati, e il rischio di obsolescenza o inconsistenza;
- le normative e i requisiti di conformità applicabili ai dati, come il GDPR o altre leggi specifiche del settore.

In base a questi criteri, **è possibile assegnare un livello di importanza e criticità a ogni dato, da basso a alto, e definire delle politiche di backup e restore adeguate a ogni livello**.
Ad esempio, i dati più critici potrebbero richiedere un backup a intervalli molto brevi, su supporti diversificati e geograficamente separati, con un alto grado di protezione, e un tempo di ripristino molto rapido. I dati meno critici potrebbero invece essere oggetto di backup meno frequenti e su supporti più economici, con un tempo di ripristino più lungo.

Questa analisi permette di ottimizzare l'uso delle risorse e di garantire una protezione adeguata a ogni tipo di dato, evitando approcci "one size fits all" che comportano costi eccessivi o compromessi sulle funzionalità.

Backup di ambienti Cloud SaaS

Nelle strategie di backup è importante includere anche i dati dei servizi Cloud di tipo SaaS – Software as a Service, ad esempio Microsoft 365, Google Workspace, Salesforce, etc.
Questi servizi, infatti, contengono dati di fondamentale importanza per l'organizzazione, ma offrono delle politiche di backup basiche, che risultano spesso troppo limitate per le esigenze aziendali e laboriose da utilizzare in caso di necessità.

Un altro aspetto da considerare è l'opportunità di conservare una copia di questi dati al di fuori della piattaforma che eroga il servizio, sia per ragioni di sicurezza che per garantirsi la proprietà dei dati indipendentemente dal fornitore del servizio stesso.

Le ormai numerose soluzioni per il backup dei dati dei servizi Cloud SaaS si dividono in due categorie:
- soluzioni "install and manage", controllate dall'IT dell'azienda, che prelevano i dati dagli ambienti Cloud e li salvano su sistemi on premise del cliente;
- soluzioni "as a service" che salvano i dati su un diverso ambiente Cloud.

Le soluzioni di tipo on-premise hanno in genere costi di licenza più bassi ma richiedono all'azienda di usare le proprie risorse per il salvataggio, il trasferimento e la manutenzione del sistema, con conseguenti costi aggiuntivi.

Le soluzioni di tipo Cloud hanno costi di licenza più elevati, che dipendono dal numero di utenti del servizio SaaS e/o dalla quantità di dati, ma, funzionando in modalità "cloud-to-cloud", non usano le risorse dell'azienda **e sono più semplici da gestire**.

È inoltre possibile costruire soluzioni ibride, ad esempio configurando una soluzione di tipo "install and manage" in modo che salvi i dati dei backup su uno storage "as a service".

Backup di ambienti Cloud IaaS e PaaS

Molte aziende hanno scelto di usare piattaforme Cloud del tipo IaaS – Infrastructure as a Service e PaaS – Platform as a Service, come per esempio Microsoft Azure, Amazon AWS, Google Cloud Platform e altre.

Queste piattaforme permettono di gestire carichi di lavoro con un modello a pagamento per uso, usufruendo di infrastrutture molto affidabili, scalabili e distribuite geograficamente.

Anche se **queste piattaforme garantiscono livelli elevati di continuità e integrità dei dati**, in genere migliori di quelli che le aziende possono raggiungere con le proprie infrastrutture on-premise, **il backup dei dati è comunque indispensabile e rientra nelle responsabilità dell'azienda cliente**.

Le piattaforme Cloud non consentono il controllo totale dell'infrastruttura sottostante, che è di proprietà del Cloud Provider, perciò non si possono usare le stesse funzionalità di backup che si usano per le infrastrutture on-premise e bisogna scegliere soluzioni specifiche che assicurano la compatibilità con la piattaforma Cloud.

Le soluzioni di backup fornite dai Cloud Provider stessi sono integrate by design con la loro piattaforma, ma si deve valutare se usare queste o altre opzioni in base a diversi fattori.

I fattori dei quali occorre tenere conto nella scelta delle soluzioni più idonee per il backup sono:

Modalità di gestione: potrebbe essere necessario monitorare separatamente la soluzione di backup del Cloud provider da quella usata per i dati on premise; se poi si usano più Cloud provider, la gestione diventa più complessa e manca una visione globale.

Destinazione dei backup: le soluzioni di backup dei Cloud provider spesso mantengono i dati nella propria piattaforma, magari trasferendoli in un altro loro datacenter per motivi di sicurezza; con una soluzione di terze parti invece si può scegliere una destinazione separata dalla piattaforma Cloud di produzione.

Integrazione con soluzioni PaaS: spesso gli ambienti PaaS non supportano soluzioni di backup diverse da quelle offerte dal Cloud provider, che rappresentano quindi l'unica opzione disponibile.

Opzioni di ripristino: le soluzioni di B&R dei Cloud provider consentono il ripristino solo all'interno della propria piattaforma, eventualmente in un altro datacenter, mentre soluzioni di terze parti possono permettere il ripristino verso infrastrutture on-premise o altri Cloud provider.

Costi: non sempre è facile confrontare i prezzi delle varie soluzioni di backup ma il backup rappresenta una componente significativa del costo di una infrastruttura ed è quindi necessario considerare questo aspetto.

Va infine tenuto conto del fatto che **le aziende sono in continua trasformazione quindi, a parità di funzionalità e caratteristiche di protezione, sono da privilegiare investimenti che permettono di adattarsi a diversi scenari con flessibilità**.

Backup su storage immutabile

Per migliorare le prestazioni e rendere meno onerose le operazioni dei sistemi di backup, da tempo si usano anche dei repository di backup basati su disco, oltre ai più classici sistemi a nastro. Tuttavia, questi sistemi sono esposti ai rischi degli attacchi informatici perché, a differenza di quanto succede con i nastri, i media non possono essere separati fisicamente dal sistema e sono quindi sempre online e alterabili o eliminabili da un hacker.

Per ovviare a questo problema **sono stati introdotti sistemi storage con immutabilità**.

Questa soluzione impedisce la corruzione o la cancellazione dei dati di backup, anche da parte dell'amministratore di sistema, fino a una data di scadenza impostata.
Il software di backup permette di governare lo storage immutabile, definendo le politiche di protezione e conservazione dei dati.

Una volta superata la data di scadenza, i dati possono essere rimossi in modo da liberare spazio per i backup successivi, mantenendo solo i punti di ripristino richiesti dalle esigenze dell'organizzazione.

Ci sono diverse tecnologie possibili per implementare questa soluzione, sia su ambienti on-premise che Cloud. Per scegliere la tecnologia migliore bisogna considerare vari aspetti come la quantità di dati da archiviare, le prestazioni, i costi di acquisto e di manutenzione, la compatibilità con l'infrastruttura hardware e software esistente.

Backup tramite copie istantanee

In molte infrastrutture on-premise i dati sono memorizzati su sistemi storage centralizzati che offrono funzionalità di copie istantanee dei volumi senza occupare troppo spazio e senza degradare le prestazioni. Queste copie di dati non sono visibili dai server o dalla rete aziendali e risultano quindi inaccessibili e non modificabili dai malware.

Grazie all'integrazione con le principali applicazioni e sistemi operativi come Oracle, SAP, Microsoft SQL Server, Windows Server e Vmware, **i dati contenuti in queste copie possono essere resi "consistenti"**, cioè logicamente coerenti per l'applicativo o sistema operativo in questione e quindi ripristinabili direttamente senza necessità di operazioni di ricostruzione o riparazione.

Grazie al fatto che queste copie si trovano già sullo storage di produzione, questa soluzione offre la possibilità di riportare in pochi secondi i dati ad una situazione temporale precedente, minimizzando sia i tempi di ripristino (RTO – Recovery Time Objective) che la perdita di dati (RPO – Recovery Point Objective).

Poiché consuma spazio storage "pregiato" sul sistema di produzione, **questa soluzione comporta dei costi relativamente alti e va quindi applicata solo alle applicazioni più critiche per il business aziendale**. Di conseguenza l'applicazione di questa soluzione può richiedere una riorganizzazione dei dati all'interno del sistema storage, con conseguenti considerazioni su prestazioni e capacità.

È inoltre importante osservare che **questa soluzione non protegge dal guasto hardware del sistema storage su cui sono conservate le copie istantanee, che potrebbe comportare la perdita di tutti i punti di ripristino. Per questo motivo, è comunque necessario integrare questa soluzione con altre forme di backup**.

Copie off-site dei dati

Per garantire la disponibilità dei dati anche in caso di perdita completa del sito di produzione, ad esempio per un incendio o una calamità naturale, è opportuno avere una copia dei dati in una diversa locazione. Il tradizionale sistema di ottenere questo risultato tramite copie su nastro e trasferimento dei nastri in una diversa sede viene oggi sempre più spesso sostituito da copie dei dati effettuate via Internet, su Cloud o altre sedi aziendali.

In tutti i casi è fondamentale assicurarsi che i dati copiati siano effettivamente ripristinabili, cioè che siano disponibili tutte le informazioni necessarie per consentire al software di backup di leggere i dati, con eventuale crittografia, e ricostruirne la struttura logica. È importante inoltre garantire la sicurezza di questi dati, sia in caso di accessi non autorizzati favoriti dal trovarsi in una sede con minori controlli, sia per evitare che infezioni avvenute nella sede principale si estendano anche alla sede secondaria. Inoltre, in caso di copie dei dati via internet, è importante assicurarsi che la connessione di rete sia sufficiente a consentire il trasferimento della mole di dati generata dai backup nei tempi richiesti dai requisiti di RPO.

Quando si ha una **combinazione di sistemi on-premise e su Cloud, i dati possono essere copiati off-site in modo incrociato, sfruttando così la disponibilità degli ambienti esistenti e la potenza di calcolo di entrambi per possibili ripristini urgenti in una soluzione di Disaster Recovery**.
Un'altra possibilità è quella di usare come destinazione dei dati replicati una località diversa, con lo scopo di assicurare la massima protezione dei dati di backup tramite una maggior separazione dalle reti di produzione.

Test e orchestrazione dei Restore

Non esiste una soluzione di B&R perfetta e infallibile, che possa garantire che i backup non siano mai incompleti, corrotti o inaccessibili a causa di errori umani, problemi tecnici, attacchi hacker o mancata osservanza delle politiche di conservazione. Quindi, è fondamentale testare con frequenza il buon funzionamento dei backup, facendo delle simulazioni di recupero dei dati a campione e per le diverse categorie. In questo modo, si potranno rilevare eventuali anomalie e controllare le performance di RPO e RTO, oltre a rendere il personale IT più abituato a fare le operazioni di restore e quindi più veloce in caso di reale bisogno.

Esistono soluzioni che facilitano le aziende in questo compito, perché permettono di automatizzare in gran parte le prove di ripristino e di creare e documentare i piani di ripristino in modo da fare le operazioni nell'ordine giusto, recuperando prima le componenti che sono necessarie per le altre e dando priorità ai dati più rilevanti.

Coordinamento tra Backup e Cybersecurity

Il sistema di backup può essere una delle fonti di informazione che aiuta chi si occupa della sicurezza informatica a capire che è in corso un attacco o si è stati infettati da un malware.

Ad esempio, se il software di backup rileva una variazione anomala del volume o della frequenza dei dati da proteggere, potrebbe significare che qualcosa non va nel sistema di produzione.

Allo stesso modo, se il software di backup segnala degli errori o dei rallentamenti nel trasferimento dei dati, ciò potrebbe indicare la presenza di un ostacolo o di un intruso nella rete. In questi casi, il team della sicurezza informatica dovrebbe essere subito allertato per investigare la situazione.

D'altro canto, il team della sicurezza informatica può aiutare chi si occupa di backup ad identificare eventuali punti di ripristino che contengono malware e a proteggere l'ambiente di backup tramite isolamento dalla rete di produzione e controllo del traffico. In questo modo, si evita che i dati di backup vengano contaminati o compromessi da un attacco in corso o da una minaccia latente e che i restore reintroducano il malware nel sistema di produzione.

Conclusioni

La necessità di adattare e potenziare le soluzioni di backup e restore è diventata una priorità ineludibile. Le nuove sfide, quali l'aumento esponenziale del volume dei dati, la complessità delle infrastrutture IT, e la sofisticazione degli attacchi informatici, richiedono approcci innovativi per garantire la sicurezza e la continuità operativa.

Il mercato risponde a queste esigenze offrendo una gamma di soluzioni avanzate, da quelle basate sul cloud a quelle che integrano l'intelligenza artificiale, per una gestione dei dati più agile, sicura ed efficiente.

Le aziende che saranno proattive nell'adottare queste tecnologie, personalizzandole in base alle proprie specificità e vulnerabilità, non solo rafforzeranno la propria resilienza in caso di disastri o attacchi informatici, ma si doteranno anche di un considerevole vantaggio competitivo. La capacità di ripristinare rapidamente le operazioni aziendali minimizzando le interruzioni è fondamentale in un'economia che valorizza l'agilità e la continuità.

In conclusione, la riconsiderazione delle strategie di backup e restore è un passo critico per le aziende che mirano a navigare con successo nel panorama digitale contemporaneo. Investire in soluzioni di B&R all'avanguardia non è più un'opzione, ma una necessità per chi aspira a mantenere la propria leadership di mercato e proteggere il proprio patrimonio informativo nel lungo termine.

Surftech

Fondata nel 2008, guida le aziende nell'innovazione con soluzioni IT avanzate e personalizzate. Si distingue per la capacità di adattare tecnologie come AI, cloud e datacenter alle specifiche esigenze dei clienti, rendendo l'IT un pilastro della loro trasformazione digitale.

Contatti

+39 045 5117703

info@surftech.it

www.surftech.it